STRATEGY RESEARCH PROJECT

PROTECTING U.S. FACILITIES: A FRAMEWORK FOR DEFENSE

BY

LIEUTENANT COLONEL MARK M. HENNES
United States Army

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Protecting U.S. Facilities: A Framework for Defense

by

LTC Mark M. Hennes
Field Artillery

COL James Thomas
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: LTC Mark M. Hennes

TITLE: Protecting U.S. Facilities: A Framework for Defense

FORMAT: Strategy Research Project

DATE: 28 February 2002 PAGES: 29 CLASSIFICATION: Unclassified

By executive order on 8 October 2001, President George W. Bush established the Office of Homeland Security, and directed six primary functions for that Office to coordinate for the executive branch. Within the function of protecting the US and its critical infrastructure from the consequences of terrorist attack is the sub-function of developing criteria for reviewing whether appropriate security measures are in place at major public and privately owned facilities. This paper examines this sub-function by exploring possible threats to domestic facilities, recommending a framework for evaluating security adequacy, and determining if DoD has a role within this framework.

TABLE OF CONTENTS

ABSTRACT iii

PROTECTING U.S. FACILITIES: A FRAMEWORK FOR DEFENSE 1

THE NEW TERRORISM 1

TERRORIST WAYS 3

HOMELAND SECURITY STRATEGY 4

SIX ELEMENTS OF A SECURITY FRAMEWORK 7

DETER 8

PREEMPTION 8

INTERDICT 10

MITIGATION 11

RECOVERY 11

REHEARSAL 12

LEGAL IMPLICATIONS 13

APPLICATION 14

CONCLUSION 15

ENDNOTES 17

BIBLIOGRAPHY 21

PROTECTING U.S. FACILITIES: A FRAMEWORK FOR DEFENSE

The attacks of September 11th, 2001 have forever shattered the illusion that Americans are safe from devastating terrorist attacks on US soil. These attacks heralded a new era in the defense of the US homeland and prompted a discussion as to how the US government should organize to execute that defense. On 8 October 2001, President George W. Bush established the Office of Homeland Security by executive order. Among the many tasks he gave to that office, President Bush charged it with protecting the US and its critical infrastructures by developing criteria for reviewing whether appropriate security measures are in place at major public and privately owned facilities. This research project explores the possible threats to domestic facilities and examines some strategic frameworks for Homeland Security, analyzing their application as a national framework for evaluating facility security adequacy. Additionally, this project examines the role of Department of Defense (DOD) assets within this framework. Before reviewing these frameworks, we must examine the threat of terrorism and likely attacks against facilities.

THE NEW TERRORISM

Viewed from a national security perspective, terrorism is an unconventional form of warfare to achieve a political goal. One could think of terrorism as a form of psychological warfare in which the killing of a small number of people convinces the rest of us that we are next in line.[1] This means that not only is the physical attack important to the terrorist, but the psychological effect is also important for the effect it has on the American psyche. The terrorist believes that attacking the American populace's sense of well being will put pressure on policy makers to change course. Therefore, we must aim our defense measures at defeating the physical attack, as well as reassuring the American public that the terrorist will ultimately be defeated.

Many noted terrorism experts believe that this is a new form of terrorism and that the US government response to this new terrorism must be new and innovative as well. They argue that the terrorists' networks are larger, more amorphous than before and that the scope of their operations is huge and ambitious. They also argue that the traditional instruments of US power, such as economic sanctions and military force, will be of little use against these networks. To defend against these new threats, the experts call for a dynamic, innovative response that is able to adapt to these new and future threats.[2] Some argue that the traditional bureaucratic structure of the federal government is incapable of rapidly adapting to this new threat, and they recommend a new, decentralized and networked interagency structure to organize US federal

efforts.[3] This challenge to the federal government to respond in a timely, innovative manner is not new. In 1997, the President's Commission on Infrastructure Protection recommended a "new mindset of adaptive protection" to respond to this new terrorism.[4]

In adapting US government policies towards terrorism, some have argued that the US should reconsider its 'no-concessions' policy. Simply put, this policy states that the US government will not negotiate with terrorists or succumb to their threats. Some terrorism experts argue that this policy does not take into account the huge consequences resulting from today's terrorists having access to weapons of mass destruction. They argue that the cost of noncompliance with terrorist demands is far greater than the short-term costs of compliance. They believe that the US government could 'keep book' on the terrorists and strike back at a later date.[5]

Other terrorism experts argue the exact opposite. They believe that the US should not give in to terrorism. To do so would only serve to reward terrorists and further their cause. Not complying with terrorist demands maintains a consistent policy and serves to keep the risks of terrorism high, thereby contributing to deterrence.[6] As will be discussed later, a strong, well-articulated policy of deterrence is a key component of the strategy for the war on terrorism.

The implications of this new terrorism on the formulation of a security framework are that the framework must yield defenses that can withstand an attack and serve to reassure the American public that they are safe. These two goals appear related, since many visible security measures can serve this dual purpose: for example strong barricades and armed guards serve to defend a facility and provide a visible sign that security measures are in place. However, such security measures can adversely affect the popular psyche by creating a 'fortress-America' appearance at public facilities. Likewise, if the defenses fail to stop an attack, America's sense of well-being can be doubly affected from the attack itself as well as from the sense of vulnerability the attack engenders. Additionally, as noted above, the new terrorism requires a constant evaluation of the threat and a dynamic response to evolving threats. Concrete barriers can protect against certain threats, but not against all of them and not against terrorists who develop new ways to thwart them. Furthermore, we can expect new threats to emerge as the terrorists adapt and respond to new defenses, so any framework must be continually evaluated and updated as terrorist tactics evolve. If the new terrorism is an adaptation, let us examine in more detail some of the new ways that terrorists attack before looking at our responses.

TERRORIST WAYS

Terrorists attack public and private facilities in a variety of ways. First, terrorists can attack a facility merely by communicating a threat, with or without the intent of actually attacking the facility. If the US government deems the threat credible, then federal authorities will notify state and local officials. These officials must then weigh the threat against available resources and possible consequences in order to respond. For example, Governor Gray Davis of California heightened security at the Golden Gate Bridge after federal authorities revealed a threat against West Coast bridges. Not only did the increased security cost the state money, but the traffic delays resulted in productivity losses for San Francisco businesses.[7] Similarly, the increased security at US-Canadian border crossing points has adversely affected the US automobile manufacturing industry due to the delay in sub-components arriving from Canadian manufacturers.[8]

In addition to this economic cost, some officials believe that increasing security levels or awareness too high or too often may also advance the terrorists' goals. In the wake of the September 11th attacks, there have been three nationally publicized terrorist warnings. Numerous mayors have stated their desire to avoid unnecessarily panicking their citizens.[9] This erosion of the popular sense of well-being may further the terrorists' goal of waging psychological warfare. However, policy makers must weigh these costs against the risks of not increasing security in the face of a credible threat.

A second means of attack that terrorists use is the intrusion of a site with the intent of either collecting information or rehearsing a future attack. This intrusion can be either the entering of a physical site, or it can be the electronic entrance (hacking) into a cyber network. For example, there is evidence that just prior to an electronic attack on a computer network, there is a substantial and noticeable increase in reconnaissance or scanning of the network.[10] This reconnaissance could be aimed at assessing weaknesses, gathering information for a future attack on that or another interdependent system, or rehearsing a future attack.

A third method that the terrorists can use to attack is the actual disruption of a facility or infrastructure. Terrorists can gain access to a target site and disrupt the operations to produce potentially catastrophic effects. A partial list of such facilities includes utilities, food production, transportation, communication, dams, and hospitals.[11] Disrupting one of these sites could produce adverse effects on a city or town, or could produce potentially catastrophic effects due to the disruption cascading through various interdependent systems.[12] For example, eighty percent of all food transported by rail in the US crosses either of two bridges over the Mississippi River. A moderate computer driven mishap near one of those bridges could cause

food shortages and skyrocketing prices.[13] While trucks might be able to eventually shoulder the load, there would be a disruption in efficient food delivery and an increase in costs. Similarly, disrupting an electric power distribution network in one state could affect neighboring states due to the linked distribution grid. Further compounding this problem is that fact that the degree of interdependence and, therefore the potential magnitude of the second and third order effects, is not well understood.[14]

What is understood is that there is the potential for adverse affects on the military due to these cascading effects. While there has never been a publicized case of a classified network being affected, the potential for an unclassified communications network being adversely affected due to an attack on a commercial communications network is real.[15] This could hamper deployment and operational planning during contingency operations. NATO experienced just such a disruption of its normal operations due to an attack on its unclassified computer network during the bombing of the Former Republic of Yugoslavia.[16] A particularly troubling aspect of this method of attack is that terrorists who are able to launch cyber attacks can disrupt from another part of the globe without ever physically entering the facility.

Yet another, and arguably the most devastating, way terrorists attack is through the destruction or physical attack of a facility. Terrorists physically attack a facility or network with the intent of causing death, injury, or destruction. From the terrorists' point of view, this attack is ideally done in such a way as to attract the largest media attention possible. Here the goal is not only the destruction of the physical facility, but also the diminution of the popular sense of well-being. The terrorists' goal can be to cause adverse economic impacts through the destruction of records, accounts, or files; the destruction of a building or critical network junction; or the death of a key individual. Defending the US homeland against these potential terrorist attacks requires a comprehensive, synchronized, and dynamic strategy.

HOMELAND SECURITY STRATEGY

To craft such a strategy, the federal government often turns to private think tanks for assistance. In the wake of the September 11th tragedy, three nationally renowned think tanks published their versions of a homeland security strategy. The Center for Strategic and International Studies (CSIS) published a comprehensive strategy in the book To Prevail: An American Strategy for the Campaign Against Terrorism. The authors define homeland security as prevention, deterrence, preemption, defense, and management of consequences but fail to define what these tenets mean or how they should be implemented. Their strategy outlines three broad objectives to be achieved: prevent future attacks on the United States, enhance the

protective capabilities of the United States, and improve the ability of the United States to respond to and manage the consequences of an attack.[17] In the area of facility security, the authors devote only four paragraphs to the protection of critical infrastructure to exhort the Bush administration to "include a greater emphasis on physical vulnerabilities and threats in various sectors." The authors' only concrete recommendations to accomplish this greater emphasis are to conduct new threat and vulnerability assessments and to delineate clear lines of responsibility from government agencies to the various infrastructure sectors.[18] While this strategy is a useful start point, its lack of specificity and superficial recommendations prevent it from being used as a comprehensive strategy for critical infrastructure facility security.

The Heritage Foundation published their recommendations in Defending the American Homeland: A Report of The Heritage Foundation Homeland Security Task Force. This report, which is even more general than the CSIS book, recommends that federal agencies create risk assessment programs for the private sector without describing the nature or focus of the assessments. The report also recommends that the federal government should establish lead agencies to develop "best practice" models for the private sector to conduct risk, vulnerability, and survivability assessments, but fails to describe what those "best practices" are or should be.[19] Later in the report, the authors recommend that the federal government develop a terrorism response checklist and a manual of civil defense exercises.[20] This recommendation is helpful because it includes the idea of conducting rehearsals or exercises to identify weaknesses.

In addition to being too general, the utility of the Heritage Foundation strategy is also hindered by its own political bias. The Foundation is a conservative think tank, and its strategic recommendations reflect this bias. For example, the report supports "a flexible free market as opposed to a rigid bureaucracy" to solve most homeland security problems.[21] Such evident political bias inhibits the full consideration of the various options available for homeland security. Although political considerations will eventually enter into the discussion of homeland security, they are more appropriate at the implementation of a strategy rather than at its formulation.

On its website, the Analytic Services, Inc. (ANSER) Institute for Homeland Security proposes a set of seven strategic functions that form a useful foundation for a national homeland security strategy. These functions are well defined, and serve as a fairly specific start point for developing the national framework for evaluating security adequacy. ANSER defines these strategic functions as follows:

Deterrence: the use of explicit or implicit threats to prevent an enemy from taking action. Achieving this requires convincing the enemy beforehand that he will face unacceptable

punishment or denial of his objectives. This punishment could be directed against the terrorist, his organization or the state that harbored and supported him.

Prevention: the defensive actions taken by the public and private sector to prevent attacks and the planning to mitigate the effects of those attacks.

Preemption: acting first to eliminate a terrorist group's imminent ability to take a specific action. This action could be federal and local justice officials acting domestically or our counterterrorism experts acting on foreign soil.

Crisis management: measures to identify, acquire, and plan for the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. Generally speaking, crisis management refers to measures taken to apprehend the perpetrators of the terrorist acts.

Consequence management: measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses and individuals affected by the consequences of terrorism.

Attribution: identifying the perpetrator of a specific act with the certainty required to allow for counter-action.

Retaliation: action taken against the perpetrator of a hostile act for the purpose of preempting or deterring further hostile acts. The promise of effective crisis management and consequence management to deny an aggressor the desired effects of attack, together with the promise of effective attribution and retaliation to punish those responsible for the attack itself, contributes directly to deterrence. [22]

These seven functions provide a valuable start point for analysis. First, the functions envision a secure homeland resulting from both proactive and reactive measures. The US must be prepared to take action before an attack, to build defenses, or to attack or arrest a terrorist group planning an attack. We must have a highly developed intelligence system that will correctly identify imminent credible threats for preemption or identify perpetrators for retaliation. Additionally, the US must always be aware of the possibility that some attacks will be successful, and what we must prepare responses to contain or mitigate the effects. Such preparation requires an efficient allocation of resources to the most effective means of defense.

Secondly, the framework is well-defined, but is descriptive not prescriptive. Specifically, these seven functions describe what needs to be done, but do not delineate the exact measures to be employed. Such inherent flexibility will allow agencies to develop the most effective measures possible for implementation within the framework. Furthermore, this descriptive manner allows for innovation in response to changes in terrorist tactics.

Lastly, the articulation of these functions and the development of a comprehensive strategy founded on them further the goal of winning the psychological war discussed previously. The development of such a strategy and the initiation of concrete steps toward implementation will reassure the American public that their leaders are in control and working towards a protective solution. Again, the assurance gained now will help the American people remain steadfast in the war on terrorism, even if some defenses are not completely successful and terrorist attacks occur. Most importantly for this project, these functions serve to illuminate the path towards developing a framework for facility security, as will be discussed below.

There are, however, some shortcomings to the ANSER functions as a foundation framework. First, some of the strategic functions overlap. The functions of consequence management and prevention both refer to measures taken to mitigate the effects of an attack. Similarly, retaliation and deterrence both speak to taking action that prevents further terrorist acts because the price is too high for the terrorist organization. The crossing of these functions blurs the discussion rather than clarifies it for policy makers who must create a strategy and allocate the resources to implement it.

Secondly, the separation between some of the functions is artificial. For example, attribution and retaliation are so inextricably linked that they should not be considered as separate functions. Effective retaliation depends so much on correctly identifying the attackers that to speak of attribution as a separate function is an artifice. Likewise, successful preemption relies on certain attribution of the conspirators. Although the Institute may have made these functions separate because separate communities will implement them (i.e. the intelligence community is responsible for attributing the source of the attack, while the defense or justice communities will take retaliatory or preemptive action) they are such an interdependent part of an effective strategy that their separation is not helpful.

Lastly, some of the elements are not germane to a discussion of a security framework for public and private facilities. Functions such as retaliation serve a useful purpose at the national policy level, but are not pertinent to a discussion of facility security. Thus, five of the seven ANSER functions (deterrence, prevention, preemption, crisis management, and consequence management) form the foundation of a security framework for protecting US facilities.

SIX ELEMENTS OF A SECURITY FRAMEWORK

With these five functions as a guide, a proposed framework for evaluating security should consist of six elements. These elements will be discussed in turn and will show how Department of Defense (DoD) assets could be used to implement each one. The analysis of

DoD involvement is founded on the principle that DoD is usually in a support role. This support role capitalizes on unique DoD capabilities or assets that are usually employed to support state or local agencies, or are employed under the direction of other federal entities, such as the Federal Emergency Management Agency (FEMA), the Department of Justice, or the Secret Service who would serve as the lead federal agency.[23]

DETER

Similar to the ANSER function, the proposed deterrence function refers to the active and passive measures at a facility that make it so difficult for a terrorist's attack to be successful that the terrorist decides not to attack. Examples of these measures include such physical protection as guards, barriers, standoff distances, and searches. Badging and background checks of personnel at facilities are a necessary component of deterring attacks by preventing infiltration and ensuring that security measures are not compromised.[24] These measures prevent the terrorist from getting near the target facility, thereby making it less likely that a terrorist attack will achieve the desired goal. Additionally, measures that are highly visible serve to reassure the public by giving the impression of proactive action being taken to ensure their protection.[25]

This element also refers to measures that make the attack so costly to a terrorist organization that the attack is deterred. Measures that will result in the capture or death of most of the attackers or those measures that will require the attackers to expend significant money or time to overcome them will result in deterrence. Clearly, measures that will result in the death of an attacker will deter all but the suicidal. Deterring the suicidal terrorist requires strong international cooperation to increase the risks to the state sponsors of terrorism and to the communities that sanction terrorists.[26]

DoD resources can contribute to deterrence at public and private facilities by providing a visible show of force. Soldiers can man checkpoints, e.g. at border crossings, and provide security augmentation at facilities, e.g. at airports, nuclear power plants, and sports venues. Usually these would be National Guard soldiers in a nonfederalized, or state, role and would only be provided for a limited time for either high profile events or until another source of security is in place.

PREEMPTION

Preemption refers to the direct actions to intercept or defeat a terrorist attack before it happens. For the purposes of facility security, preemptive capabilities may not be present at every, or even most, facilities. Facilities located close to one another would be protected under

an umbrella provided by local, state and federal law enforcement agencies. However, in the context of a comprehensive framework for facility protection, a certain level of preemptive capability commensurate with the risk associated with a given facility must be present, so it is included as an element of this framework. Like the ANSER function, the proposed preemption function relies on good intelligence to discern the intent and capability of a terrorist organization. At the local level, preemption occurs when the Federal Bureau of Investigation, who has the lead for domestic preemption, notifies state and local officials that an attack is imminent. This would lead to a cooperative response by federal, state, and local law enforcement agencies to defeat the terrorist attack before it happens.[27]

DoD has a substantial role in gathering intelligence and preempting attacks on foreign soil. Through the technical means of the National Security Agency and the National Imagery and Mapping Agency, DoD can provide communications intelligence and satellite imagery, respectively. These resources can provide valuable information as to the terrorists' plans and intentions, as well as the location of their training facilities and state sponsors. Comprehensive communications intelligence is important because there is a belief that the new terrorism of today is organized in widely dispersed networks. The theory is that these networks would be susceptible to detection and monitoring because the various nodes need to communicate with each other for operations and planning.[28] The success of the Al Qaeda network on September 11, 2001, shows that this theory does not hold true for every terrorist network. Through the nontechnical means of overt collection assets, such as the Defense Attaché, and covert collection assets, such as Special Operations Forces, DoD can provide a military assessment on the security and stability of other nations. These assets can provide information on nations that harbor terrorists as well as comment on the capabilities and intentions of specific groups. This information would have to be handed off to the Department of Justice if the preemptive strike were to be carried out on US soil. If the requirements exceeded federal, state, and local law enforcement capabilities, then DoD could provide assistance although it would have to be in compliance with certain legal restrictions that will be discussed below. Another way in which DoD could contribute to preemptive measures would be to provide training to improve law enforcement capabilities.[29] Although many larger cities have substantial preemptive capabilities, many mid-sized and smaller cities do not. Alternatively, if the preemptive strike were to be carried out on foreign soil, then the DoD Special Operations Forces or other military force could perform the mission. Indeed, this clear determination to use force preemptively, whether on US or foreign soil, is a necessary part of deterrence.[30]

INTERDICT

Interdiction refers to the active and passive measures at a given facility which stop an attack that is already in progress. Interdiction is not the erection of barriers to deter an attack or the preemption of an attack before it begins. It refers, rather, to those measures that stop an attack once the defensive barriers are breached and the attack is underway. While defensive barriers are an important part of comprehensive facility security, a skilled and determined terrorist may eventually penetrate them. Interdiction, therefore, is the next level of security measures that serve to halt an attack that is in progress. It includes such measures as the active monitoring of video surveillance or motion sensors to trigger an armed reaction force or the activation of barriers or other means to defeat an attack. These measures can include the installation of chemical or biological hazard monitors which sound an alarm to notify authorities.. Successful interdiction also includes the measures necessary to defeat an attack on a vulnerable cyber network. These measures include log-in monitoring, intrusion detection, anti-virus protection and ingress/egress monitoring.[31]

With the exception of protecting federal assets, DoD has a limited role here, and usually only in support of another agency. For example, DoD could provide air cover and snipers for a high profile event, or specialized skills, such as bomb detection and disposal. In fact, 10 USC 2564 specifically authorizes DoD to provide support to international sporting competitions and other special events. Such support may include physical security, aviation, logistics, communications, joint operations and command centers, and explosive ordnance disposal.[32] While many larger cities have these capabilities already, DoD could be called on to augment them, as was done during the 1996 Olympics.[33] Such support is already planned for the 2002 Olympics at Salt Lake City, Utah through the 5,000 man Joint Task Force Olympics.[34]

DoD can also support the development of interdiction measures to protect computer networks. For example, the Joint Program Office – Special Technology Countermeasures (JPO-STC) is a defensively focused organization chartered by the Under Secretary of Defense for Acquisition, Technology and Logistics. With the Navy as the Executive Service, the JPO-STC can assist federal and non-federal agencies with computer network interdiction measure development through its Infrastructure Assurance Program. This program assists customers by conducting a vulnerability assessment and helping to develop crisis response plans and specific countermeasures.[35] Although focused on supporting only DoD assets, lessons learned by the JPO-STC could support other programs aimed at critical infrastructure protection.

MITIGATION

Mitigation is the taking of active and passive measures to minimize the effects of an attack after it happens. Much like ANSER's function of Consequence Management, the proposed mitigation function refers to the reactive measures that function to contain or isolate an attack in order to limit further damage or injury. Some examples include the installation of filters and shut-down controls to limit the spread of contamination in a building through its air circulation system. Mylar sheeting can be applied to windows to minimize injury from glass shards caused by a blast.[36] To mitigate the effects of a cyber attack, critical systems or files can be backed up and routers can be programmed to limit the rate at which messages typically associated with attacks are sent throughout the network.[37]

In reacting to terrorist attacks, DoD's mitigation role is in support of local and state first responders and usually under the direction of FEMA. DoD can provide the critical skills, equipment, or manpower that exceeds the capabilities of the local and state agencies. For example, the National Guard has established highly trained, rapidly deployable Civil Support Teams (CST) to respond rapidly to terrorist attacks using chemical, biological, radiological, nuclear, or high explosive means. While not every state has a CST yet, all of the governors have the ability to call on whatever equipment, skills or manpower that their National Guard units possess.[38] These units can facilitate rapid response by having a current inventory of equipment and skill of their units, and by practicing with their local first response agencies. As noted previously, DoD could also assist by providing technical training or equipment, such as chemical-biological hazard identification and handling, to local first response agencies.

RECOVERY

Recovery refers to actions taken to repair a damaged facility or to restore a critical function to full or partial service. Unlike the ANSER functions, this element of the proposed framework is separate to highlight the need for organizing and planning prior to an attack. Recovery can be an event of long duration occurring well after the initial effects are contained and partial service restored.

FEMA is the lead federal coordinator for recovery activities after an attack. FEMA responds at the direction of the president after a request from the state governor. Governors will make such a request only when the magnitude of the emergency exceeds state and local capabilities, including those of the state's National Guard.[39] FEMA is responsible for the Federal Response Plan (FRP), which outlines the responsibilities of the various federal agencies. Within the FRP, DoD has the lead role only in the Emergency Support Function of

Public Works and Engineering (ESF 3). In this function, the Army's Corps of Engineers is the primary agency to help restore essential public services and facilities. Additionally, DoD provides support to other federal agencies that have the lead in other Emergency Support Functions.[40] Thus, DoD support to recovery operations could include the restoration of electrical power, the provision of heavy equipment to remove wreckage, the establishment of a communications network for emergency response personnel, or the helicopter transportation of critical supplies. The DoD's Joint Forces Command has a subordinate element, known as the Joint Task Force Civil Support, that is available to help organize and manage a large DoD response.[41] As noted previously, DoD support to recovery operations will be limited in scope and duration, usually only until minimal functions can be restored.

REHEARSAL

A critical element of a national framework for evaluating security that is not an explicit part of the ANSER model is the need for rehearsing response plans. Rehearsing provides the responders the opportunity to practice the response procedures and identify potential problems. It also allows them to look for gaps in the plans which terrorists might be able to exploit. Innovative solutions to these problems can be developed and incorporated into the updated response plans. Such rehearsals and exercises also bring together the various agencies required to work together under crisis conditions and affords them the opportunity to learn what resources each agency brings to a crisis.

Federally, there are a number of resources that local and state officials can draw on to devise response plans and to implement an exercise plan. For example, the Sandia National Laboratories has established a Center for Civil Force Protection to assist government and private industries in improving their security and self-protection measures. Funded by the National Institute of Justice, this center provides a virtual library of training materials that institutions can use in developing their response plans[42]. The Department of Justice also provides assistance to state and local officials through its Office of Domestic Preparedness (ODP). This office provides direct training and technical assistance on a variety of subjects of interest to those preparing response plans. For training on domestic preparedness issues, the ODP utilizes a number of institutions and private contractors to teach courses. ODP also provides technical assistance in the form of information, templates, samples, and workshops that are specifically designed to enhance local planning efforts.[43]

DoD can assist in the rehearsal of these plans by designing and executing simulations and exercises. DoD assets can be used in making vulnerability assessments, or in the conduct

of simulated terrorist attacks, complete with casualties and simulated chemical or biological hazards.[44] In fact, this is occurring already. A recent check of a DoD website showed 55 exercises in the calendar year 2002 Interagency Consequence Management Exercise Schedule.[45] The results of these exercises will need to be disseminated to other agencies for incorporation of the lessons learned into revised anti-terrorist plans.

LEGAL IMPLICATIONS

Before examining how the six elements could be applied, it is reasonable to consider a few legal implications for using DoD resources in the context of facility security missions. The Constitution authorizes the Congress to "call forth the militia" in order to execute laws, suppress insurrections, and repel invasions. The President is required by the Constitution to "take care that the laws are enforced" and he may, of course use the military to enforce those laws.[46] Statutorily, the so-called Insurrection Statutes (10 USC 331-334) authorize the President to use military forces to restore and maintain public order, to respond to requests for aid from the state governments, and to protect constitutional rights under certain conditions. The President is also authorized to use military forces to protect federal property and functions by 18 USC 231 and 1361 and by 50 USC 797.[47]

However, federal military forces are generally prohibited from directly enforcing civil laws by the Posse Comitatus Act, codified in 18 USC 1385. Enacted by Congress in the wake of certain excesses by federal troops during the post-Civil War reconstruction period, this Act was an effort to prevent the abuse of federal authority. Although this Act only includes Army and Air Forces, by DoD policy Navy and Marine Corps assets are now included. The practical effect of this Act is that Active Component military, and National Guard personnel when serving in a federal capacity, cannot enforce laws or arrest violators. It is important to note that National Guard soldiers serving in a state capacity would be permitted to do so. As noted above, the Insurrection Statutes are an important exception to this Act so that federal troops, when acting under the power of the president to quell domestic disturbances, are allowed to enforce laws and restore order. Additionally, it has been determined that passive support to law enforcement, such as aerial photographic and visual search and surveillance by military personnel, does not violate the Act.[48]

The Fiscal Year 1997 appropriation provided for an additional use of DoD resources in a domestic role. Known as the "Defense Against Weapons of Mass Destruction (WMD) Act of 1996", or the Nunn-Lugar-Domenici Act, it required DoD to train state and local first responders to handle the consequences of WMD incidents. Additionally, DoD was authorized to support the

Department of Justice in emergencies involving chemical or biological WMD. Lastly, the Act required the DoD to maintain a rapid response team to respond to WMD incidents. Later legislation transferred the mission of training state and local first responders to the Department of Justice.[49] The Fiscal Year 1999 appropriation further clarified the use of military forces in the remaining WMD missions to specifically include the use of Reserve Component personnel.[50]

Thus the existing laws do not unduly inhibit the use of DoD assets in the framework for facility security. Although the Posse Comitatus Act prohibits the use of Active Component forces in a strictly law enforcement role, since they are generally not trained for this mission anyway, this prohibition is not burdensome. Additionally, the prohibition does not apply to National Guard personnel while functioning in a state role, so these forces would be available to the state governor if law enforcement missions needed to be done.

APPLICATION

With the six elements of the proposed framework in mind, let us briefly examine how they could be applied to assess the security adequacy at US facilities. First, as recommended by CSIS and the Heritage Foundation, the federal government must delineate which agencies are responsible for which critical infrastructure sectors. These agencies, then, would be responsible for applying the six elements to create detailed criteria for the facilities in their areas of responsibility. For example, it is reasonable for the Department of Energy to be responsible for developing detailed checklists to evaluate the security adequacy at public power utilities. In this way, operators of nuclear and electric power plants would receive checklists written in terms of their facilities that allow them to evaluate their security posture. Similarly, the Department of Transportation would apply the framework to develop evaluation criteria for airport and seaport security. The Department of Justice, which already has the mission to train state and local officials, would integrate this framework into their training plans. In this way, these officials would evaluate public buildings and assist with the assessments of public facilities in their jurisdiction.

The Department of Justice could also help promulgate the framework by sponsoring seminars focused on critical infrastructure protection. Invitees to these seminars could include both public and private security professionals who could discuss and further refine the application of this framework. These seminars would also encourage private contractors to include the framework in their assessments of facilities, and would allow federal, state, and local officials to learn what works in private sector security. This information sharing is an important part of updating security measures as terrorist tactics evolve.

Cyber protection is more difficult because nearly all critical infrastructures depend upon computer networks to function. Therefore cyber protection affects all of the sectors of responsibility. To overcome this problem, each department should include cyber protection criteria within each of their checklists. Since the departments are already responsible for protecting their own networks, they have resident expertise that could implement these same measures within their facility protection checklists. Additionally, the federal government should disseminate the framework to software developers and encourage them to include the principles in future software developments.

Local, state, and federal officials could evaluate the implementation of this framework through exercises and assessments, which they would use to prioritize spending to fix the problems. While the framework does not help prioritize solutions, it does provide a comprehensive picture of the problems for elected officials to set the priorities. Solutions to these problems could include federal or state grants for equipment or training, as well as requests for DoD assistance. As noted in the development of the framework, DoD assets can be used in a variety of ways to help address problems.

CONCLUSION

The six elements for evaluating the effectiveness of security at public and private facilities provide a flexible foundation for the protection of critical US facilities. Similar to the ANSER Institute's seven functions, the facility framework incorporates the aspects of proactive and reactive measures in preparing response measures. Both aspects are necessary in working towards comprehensive facility protection in order to respond to the terrorists before and after they strike. These elements are also broad enough in definition to allow for innovation as terrorist's change their methods. Furthermore, articulating a framework for protecting such facilities will go along way towards inoculating the American public against the future psychological warfare of another terrorist attack.

Department of Defense assets can have pivotal roles within this framework for protecting US facilities. As providers of critical skills, manpower, and equipment, DoD can assist in deterring and preempting attacks before they happen, or in the mitigation and recovery after an attack. Most important, DoD resources can be used in assisting the critical element of rehearsing response plans. However, policymakers must be cognizant of the possibility of overusing DoD assets to the detriment of their warfighting capability. While DoD has a number of assets and a variety of skills, its primary task remains being capable of fighting wars.

Although, when used in support of other federal, state, and local authorities within this framework, DoD assets can contribute significantly to facility protection.

WORD COUNT = 6497

ENDNOTES

[1] Ehud Sprinzak, "The Great Super Terrorism Scare," Foreign Policy (Fall 1998); database on-line; available from UMI-ProQuest, Bell and Howell; accessed 5 November 2001.

[2] This discussion of the new terrorist threat was summarized from Bruce Hoffman, "Forward," in The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, eds. James M. Smith and William C. Thomas (USAF Academy, CO: USAF Institute for National Security Studies, 2001), viii to xiv.

[3] David Tucker, "Combating International Terrorism," in The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, eds. James M. Smith and William C. Thomas (USAF Academy, CO: USAF Institute for National Security Studies, 2001), 140.

[4] President's Commission on Critical Infrastructure Protection, Critical Foundations (Washington, D.C.: U.S Government Printing Office, October 1997), 23.

[5] Tucker, 148.

[6] Sprinzak, "The Great Super Terrorism Scare".

[7] Pam Belluck and Timothy Egan, "Cities and States Say Confusion and Cost Hamper Security Drive," New York Times 10 December 2001; available from <http://ebird.dtic.mil/Dec2001/e200111210cities.htm>; Internet; accessed 11 December 2001.

[8] An Air National Guard Major General related this information about the effect of increased border crossing security in seminar at the U.S. Army War College.

[9] Belluck.

[10] Michael A. Vatis, Cyber Attacks During the War on Terrorism: A Predictive Analysis (Hanover, NH: Institute for Security Technology Studies at Dartmouth College, 2001), 19.

[11] David H. Freedman, "Information Warfare," Technology Review November 2001; available from <http://www.techreview.com/magazine/nov01/print_version/freedman.html>; Internet; accessed 26 October 2001, 2.

[12] U.S. Commission on National Security/21st Century, Roadmap for National Security: Imperative for Change, (Washington, D.C.: U.S. Government Printing Office, 15 March 2001), 12.

[13] Freedman, 2.

[14] Vatis, 7.

[15] Freedman, 2.

[16] Although there is no published evidence that these attacks adversely affected the bombing campaign, it is known that the cyber attacks curtailed normal operations until the networks could be restored. Vatis, 7.

[17] Summarized from Kurt M. Campbell and Michele A. Flournoy, To Prevail: An American Strategy for the Campaign Against Terrorism (Washington, D.C.: Center for Strategic and International Studies Press, 2001), 107-110.

[18] Ibid., 114.

[19] Paul Bremer, III and Edwin Meese, III, Defending the American Homeland: A Report of The Heritage Foundation Homeland Security Task Force (Washington, D.C.: The Heritage Foundation, January 2002), 24.

[20] Ibid., 37.

[21] Ibid., 24.

[22] Randy Larsen, Dave McIntyre, and Mark DeMier, "A Primer on Homeland Security: Definitions of Strategic Functions;" available from <http://www.homelanddefense.org/bulletin/definitions.htm>; Internet; accessed 10 December 2001.

[23] James H. Thomas, "Chapter 23: Military Assistance to Civilian Authorities," in How the Army Runs: A Senior Leader Reference Handbook, ed. Edward J. Filiberti (Washington, D.C.: US Government Printing Office, 2001), 23-17.

[24] Sharon Begley, "Protecting America: The Top 10 Priorities," Newsweek 5 November, 2001; available from <http://ebird.dtic.mil/oct2001/s2001/029priorities.htm>; Internet; accessed 29 October 2001.

[25] Ehud Sprinzak, "Rational Fanatics," Foreign Policy (September/October 2000); database on-line; available from UMI-ProQuest, Bell and Howell; accessed 5 November 2001, 72.

[26] Sprinzak believes that suicidal bombers can be deterred by increasing the risks to those that sanctioned the attacks. Although Israel has had only limited success in its efforts to retaliate, one wonders how many attacks there would have been had these measures not been taken. Ibid.

[27] Robert M. Blitzer, "Domestic Preemption," in The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, eds. James M. Smith and William C. Thomas (USAF Academy, CO: USAF Institute for National Security Studies, 2001), 122-125.

[28] Tucker, 134.

[29] R. W. Madden, Achieving Unity of Effort: A Challenge in Domestic Support Operations, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 9 March 1998), 11.

[30] U.S. Commission on National Security, 12.

[31] Vatis, 19.

[32] James H. Thomas, 23-25.

[33] Madden, 29.

[34] A speaker in the AY 2002 Commandant's Lecture Series, US Army War College, provided this information on JTF Olympics.

[35] This information on the mission and capabilities of the Joint Program Office – Special Technology Countermeasures was summarized from "Joint Program Office – Special Technology Countermeasures;" available from <http://www.nswc.navy.mil/iap>; Internet; accessed 3 January 2002.

[36] Begley.

[37] Vatis, 20.

[38] Thomas, 23-25.

[39] Ibid, 23-21.

[40] Ibid., 23-15 and 23-16.

[41] Rand Corporation, Preparing the US Army for Homeland Security, (Arroyo, AZ: RAND Arroyo Center, September 1999), 72.

[42] John German, "Press Release: Sandia to Provide One-stop Terrorism Readiness Help to Communities Through National Institute of Justice Virtual Center," 30 March 2000; available from <http://www.sandia.gov/media/newsrelease/nr2000/ccfp.htm>; Internet; accessed 3 November 2001.

[43] This information on the Justice Department's Office of Domestic Preparedness was summarized from "Office of Domestic Preparedness;" available from <http://www.ojp.usdoj.gov/odp/ta/ta.htm>; Internet; accessed 3 November 2001.

[44] U.S. Commission on National Security, 12.

[45] "Interagency Consequence Management Exercise Schedule," 3 December 2001; available from <http://www.doms.pentagon.mil/exercises/exercise_schedule.htm>; Internet; accessed 10 December 2001.

[46] These Constitutional bases for the use of the military were taken from a Noontime Lecture at the U.S. Army War college.

[47] These statutory authorizations for the Presidential use of military force were summarized from The Joint Chiefs of Staff, Joint Tactics, Techniques, and Procedures for Antiterrorism, Joint Pub 3-07.2 (Washington, D.C.: The Joint Chiefs of Staff, 17 March 1998), III-4 and 5.

[48] These aspects of the Posse Comitatus Act were summarized from RAND, 243-245.

[49] RAND, 73.

[50] William C. Thomas, "The Military's Response to Domestic WMD Terrorism," in The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, eds. James M. Smith and William C. Thomas (USAF Academy, CO: USAF Institute for National Security Studies, 2001), 180.

BIBLIOGRAPHY

Begley, Sharon. "Protecting America: The Top 10 Priorities." Newsweek November 5, 2001. Available from <http://ebird.dtic.mil/oct2001/s2001/029priorities.htm>. Internet. Accessed 29 October 2001.

Belluck, Pam and Timothy Egan. "Cities and States Say Confusion and Cost Hamper Security Drive." New York Times 10 December 2001. Available from <http://ebird.dtic.mil/Dec2001/e200111210cities.htm>. Internet. Accessed 11 December 2001.

Blitzer, Robert M. "Domestic Preemption." In The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, eds. James M. Smith and William C. Thomas, 121-128. USAF Academy, CO: USAF Institute for National Security Studies, 2001.

Bremer, Paul, III and Edwin Meese, III. Defending the American Homeland: A Report of The Heritage Foundation Homeland Security Task Force. Washington, D.C.: The Heritage Foundation, January 2002.

Campbell, Kurt M. and Michele A. Flournoy. To Prevail: An American Strategy for the Campaign Against Terrorism. Washington, D.C.: Center for Strategic and International Studies Press, 2001.

Cilluffo, Frank J., Charon C. Cardash, and Gordon N. Lederman. Combating Chemical, Biological, Radiological, and Nuclear Terrorism: A Comprehensive Strategy. Washington, D.C.: Center for Strategic and International Studies, May 2001.

Echevarria, Antulio J. II. The Army and Homeland Security: A Strategic Perspective. Carlisle Barracks: U.S. Army War College Strategic Studies Institute, March 2001.

Freedman, David H. "Information Warfare." Technology Review November 2001. Available from <http//www.techreview.com/magazine/nov01/print_version/freedman.html>. Internet. Accessed 26 October 2001.

German, John. "Press Release: Sandia to Provide One-stop Terrorism Readiness Help to Communities Through National Institute of Justice Virtual Center." 30 March 2000. Available from <http://www.sandia.gov/media/newsrelease/nr2000/ccfp.htm>. Internet. Accessed 3 November 2001.

Hoffman, Bruce. "Foreward." In The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, eds. James M. Smith and William C. Thomas, i-xxi. USAF Academy, CO: USAF Institute for National Security Studies, 2001.

"Interagency Consequence Management Exercise Schedule." 3 December 2001. Available from <http://www.doms.pentagon.mil/exercises/exercise_schedule.htm>. Internet. Accessed 10 December 2001.

Johnston, Stanley W., Jr. Domestic Support Operations: Military Roles, Missions, and Interface with Civilian Agencies. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 26 March 1997.

"Joint Program Office - Special Technology Countermeasures ." Available from <http://www.nswc.navy.mil/iap>. Internet. Accessed 3 January 2002.

Larsen, Randy and Dave McIntyre. "A Primer on Homeland Security: Strategic Functions, Threats and Mission Areas." Available from <http://www.homelandsecurity.org/bulletin/strategic_functions.htm>. Accessed 3 November 2001.

Larsen, Randy, Dave McIntyre, and Mark DeMier. " A Primer on Homeland Security: Definitions of Strategic Functions." Available from <http://www.homelanddefense.org/bulletin/definitions.htm>. Accessed 10 December 2001.

Madden, R. W. Achieving Unity of Effort: A Challenge in Domestic Support Operations. Strategy Research Project. Carlisle Barracks: US Army War College, 9 March 1998.

McIntyre, Dave. "Winning This One --- The Logic of Homeland Security." Available from <http//www.homelandsecuriyt.org/bulletin/primer_winningthisone.htm>. Internet. Accessed 3 November 2001.

"Office of Domestic Preparedness." Available from <http://www.ojp.usdoj.gov/odp/ta/ta.htm>. Internet. Accessed 3 November 2001.

Paulson, Amanda. "City by City, Terror War Goes Local." The Christian Science Monitor 25 October 2001. Available from <http://www.csmonitor.com/2001/1025/p1s1-ussc.html>. Internet. Accessed 26 October 2001.

Pickering, Isaac D. Enhancing the Strategic Roles of the National Guard: Domestic Support Operations. Strategy Research Project. Carlisle Barracks: US Army War College, 7 April 1997.

President's Commission on Critical Infrastructure Protection. Critical Foundations. Washington, D.C.: U.S. Government Printing Office, October 1997.

Probst, Peter S. "Intelligence and Force Protection vs. Terrorism." In The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, eds. James M. Smith and William C. Thomas, 169-176. USAF Academy, CO: USAF Institute for National Security Studies, 2001.

RAND Corporation. Preparing the US Army for Homeland Security. Arroyo, AZ: RAND Arroyo Center, September 1999.

Roxborough, Ian. The Hart-Rudman Commission and the Homeland Defense. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, September 2001.

Smith, James M. and William C. Thomas, eds. The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors. USAF Academy, CO: USAF Institute for National Security Studies, 2001.

Sprinzak, Ehud. "The Great Super Terrorism Scare." Foreign Policy (Fall 1998): 110-119. Database on-line. Available from UMI-ProQuest, Bell and Howell. Accessed 5 November 2001.

_____ "Rational Fanatics." Foreign Policy (September/October 2000): 66-73. Database on-line. Available from UMI-ProQuest, Bell and Howell. Accessed 5 November 2001.

The Joint Chiefs of Staff. Joint Tactics, Techniques, and Procedures for Antiterrorism. Joint Pub 3-07.2. Washington, D.C.: The Joint Chiefs of Staff, 17 March 1998.

Thomas, James H. "Chapter 23: Military Assistance to Civilian Authorities." In How the Army Runs: A Senior Leader Reference Handbook, ed. Edward J. Filiberti, 23-1 to 23-31. Washington, D.C.: U.S. Government Printing Office, 2001.

Thomas, William C. "The Military's Response to Domestic WMD Terrorism." In The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, eds. James M. Smith and William C. Thomas, 179-200. USAF Academy, CO: USAF Institute for National Security Studies, 2001.

Tucker, David. "Combating International Terrorism". In The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, eds. James M. Smith and William C. Thomas, 129-154. USAF Academy, CO: USAF Institute for National Security Studies, 2001.

U.S. Commission on National Security/21st Century. Roadmap for National Security: Imperative for Change. Washington, D.C.: U.S. Government Printing Office, 15 March 2001.

Vatis, Michael A. Cyber Attacks During the War on Terrorism: A Predictive Analysis. Hanover, NH: Institute for Security Technology Studies at Dartmouth College, 2001.